Appendix 3 - Guidelines for Staff - Emailing

1. Gaining Consent

- Give the patient (or parent/guardian) the risk information leaflet "**Internet Advisory Leaflet for Patients"** and also the "**User Guide for Opening E-mails sent by the Secure NHS E-mail process**"
- For children under age 16, the parent/guardian and the child (if mature enough) should counter-sign the document
- Always give the family a photocopy of the consent form.

2. Starting to email

- Ask the patient/parent/guardian to email you first – this should not contain any personal information – is only completed as a test to ensure you get the correct e-mail address.
- From then onwards, use the instructions for sending a secure e-mail "Procedure for sending secure e-mail" (paragraph below)
- When emailing patients you must make sure that you are only sending information that the patient has approved – each service must have its own procedures in place for this – i.e. amend address contact sheet in file to include this information, written in front of file etc
- If emailing photos or videos remember to regularly delete your sent items and then your deleted mailbox so not to fill up your storage
- When sending emails to non nhs.scot a security message is contained however the following should also be added at the end of your emails – this could be done by adding it to your signature:

  "Email can be an insecure method of communication for personal information/details as it could be intercepted, corrupted, lost or destroyed. You have previously consented to our service communicating with you via email however if you would prefer to receive communication by another format please email or telephone the service."

3. Reviewing and Updating Consent

- Consent should be reviewed periodically by staff - 6 monthly – if changes are required a new form should be completed. Staff should make an entry on their clinical notes to record that the review was completed
- A new consent form should be completed every time a new request for assistance is made to the service
- If the patient is transferred to another therapist a new consent form should be signed

4. Sending [secure] email via nhs.scot to a non-secure e-mail address

Only to be used after the patient has been made aware of the risks of their medical information being sent by e-mail and consented to receiving emails.

4.1. How to send an e-mail securely

4.1.1 GREEN: Unclassified Information

This is information which is unlikely to cause distress to individuals, breach confidence, or cause any financial or other harm to the organisation. This can include information which mentions only a person's name (e.g. routine appointment confirmation letter) as long as it does not contain anything that is judged to describe a person's physical or mental state.
Note: The sensitivity level and impact can also vary depending on the volumes (e.g. a corporate document with just one name of an employee may be unclassified whereas a document with hundreds of names may push it into the amber category below).

Control for protecting 'Unclassified' (Green) Information sent by email

Action / Procedure	Information Security Requirements
Sending By Public Network (inc. Email)	Limited on a need to know basis

4.1.2 AMBER: Protected Information

In NHS Fife the largest proportion of patient information can be said to require extra protection because it constitutes sensitive personal data as defined by the Data Protection Act. In particular:

- Any information about an individual (i.e. anything clinical or non-clinical) that would cause short-term distress, inconvenience or significant embarrassment if lost.
- Any information which if lost would lead to a low risk to a person's safety (e.g. loss of an address but no evidence to suggest direct harm would result)
- Any information if lost that would be likely to negatively affect the efficiency of that service (e.g. cancellation of appointments).

Control for protecting 'Protected' (Amber) Information Sent by Email

Action / Procedure	**Information Security requirements**
1. Open the test e-mail you have previously received from the patient. In the subject header type **[secure]** then the title of your message. This must be done **with the square brackets** – or the e-mail will be sent unencrypted. ('secure' can be upper or lower case – this does not matter). 2. Make sure there is a space between [secure] and the title of your message. 3. In the main message box type in covering information to tell the recipient why you are contacting him. 4. FINALLY – put in the recipient's email address. It is important to do this last to ensure information is sent to the correct person. 5. Double-check that you are sending to the correct person. 6. Hit send.	Allowed as per section 4.5.6 of NHS email policy (GP/E6), which refers to IG and IT security approval, the need to document a Privacy impact Assessment and enforced encryption.

4.1.3 RED: Highly Sensitive Information

NHS Fife holds information which is highly sensitive. Particularly:

- Any information which if lost could directly lead to actual harm (e.g. to mental health or put the person at physical risk from themselves or others in any way).
- Any information that would in the opinion of a qualified person cause substantial distress and/or constitute a substantial breach in privacy (e.g. identity theft, loss of professional standing) to the subject. This is likely to include for example information on a person's sexual health.
- Information that affects the privacy or could cause distress to more than one individuals (e.g. several family members or several linked persons contained in a file).
- Information relating to vulnerable persons' health (e.g. child protection cases)
- Information governed by legislation that requires additional layers of security and recognises the substantial distress that would be caused by loss (e.g. embryology, human fertilisation and gender re-assignment).
- Information if lost that is likely to result in undermining confidence in the service or would cause significant financial loss to the organisation, prejudice investigation of crime etc.

Control for protecting 'Protected' (RED) Information Sent by Email

Action / Procedure	**Information Security Requirements**
Contact the Data Protection Office for further advice	**By default this is not allowed**, however there may be occasions (Court orders etc.) where the NHS is required to supply high sensitive information. The Data Protection Office should be able to provide further advice on secure means of transmission.